

New effective differential Nullstellensatz*

Richard Gustavson, Marina Kondratieva, and Alexey Ovchinnikov

CUNY Graduate Center, Department of Mathematics, 365 Fifth Avenue, New York, NY 10016, USA

rgustavson@gc.cuny.edu

Moscow State University, Department of Mechanics and Mathematics, Moscow, Russia

kondratieva@sumail.ru

CUNY Queens College, Department of Mathematics, 65-30 Kissena Blvd, Queens, NY 11367, USA

CUNY Graduate Center, Department of Mathematics, 365 Fifth Avenue, New York, NY 10016, USA

aovchinnikov@qc.cuny.edu

Abstract

We show new upper and lower bounds for the effective differential Nullstellensatz for differential fields of characteristic zero with several commuting derivations. Seidenberg was the first to address this problem in 1956, without giving a complete solution. The first explicit bounds appeared in 2009 in a paper by Golubitsky, Kondratieva, Szanto, and Ovchinnikov, with the upper bound expressed in terms of the Ackermann function. D'Alfonso, Jeronimo, and Solernó, using novel ideas, obtained in 2014 a new bound if restricted to the case of one derivation and constant coefficients. To obtain the bound in the present paper without this restriction, we extend this approach and use the new methods of Freitag and León Sánchez and of Pierce from 2014, which represent a model-theoretic approach to differential algebraic geometry.

1 Introduction

It is a fundamental problem to determine whether a system $F = 0$, $F = f_1, \dots, f_r$, of polynomial PDEs with coefficients in a differential field K is consistent, that is, it has a solution in a differential field containing K . Differential elimination [1, 10] is an effective method that can answer this question, and its implementations (including MAPLE packages) can handle examples of moderate size if a sufficiently powerful computer is used. The differential Nullstellensatz states that the above consistency is equivalent to showing that the equation $1 = 0$ is not a differential-algebraic consequence of the system $F = 0$. Algebraically, the latter says that 1 does not belong to the differential ideal generated by F in the ring of differential polynomials.

The complexity of the effective differential Nullstellensatz is not just a central problem in the algebraic theory of partial differential equations but is also a key to understanding the complexity of differential elimination. It is often the case that this leads to substantial improvements in algorithms. Let $F = 0$ be a system of polynomial PDEs in n differential indeterminates (dependent variables) and m derivation operators $\partial_1, \dots, \partial_m$ (that is, with m independent variables), of total order h and degree d . For every non-negative integer b , let $F^{(b)} = 0$ be the set of differential equations obtained from the system $F = 0$ by differentiating each equation in it b times with respect to any combination of $\partial_1, \dots, \partial_m$. An upper bound for the effective differential Nullstellensatz is a numerical function $b(m, n, h, d)$ such that, for all such F , the system $F = 0$ is

*This work was partially supported by the NSF grants CCF-0952591 and DMS-1413859.

inconsistent if and only if the system of polynomial equations in $F^{(b(m,n,h,d))}$ is inconsistent. By the usual Hilbert's Nullstellensatz, the latter is equivalent to

$$1 \in \left(F^{(b(m,n,h,d))} \right).$$

For example, in the system of polynomial PDEs

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 1 \end{cases} \quad (1.1)$$

$\partial_1 = \partial/\partial_x$, $\partial_2 = \partial/\partial_y$, and so $m = 2$, the differential indeterminates are u and v , and so $n = 2$, the maximal total order of derivatives is $h = 2$, and the maximal total degree is $d = 2$. The corresponding system of polynomial equations is

$$\begin{cases} z_1 + z_2 = 0 \\ z_3 - z_4 = 0 \\ (z_5 + z_6)^2 + (z_7 + z_8)^2 = 1 \end{cases}$$

which is consistent (e.g., take $z_1 = \dots = z_7 = 0$ and $z_8 = 1$). On the other hand, system (1.1) is inconsistent. Indeed, applying ∂_1 and ∂_2 to the first and second equations in (1.1), consider the extended system

$$\begin{cases} u_x + v_y = 0 \\ u_y - v_x = 0 \\ u_{xx} + v_{xy} = 0 \\ u_{yy} - v_{xy} = 0 \\ u_{xy} + v_{yy} = 0 \\ u_{xy} - v_{xx} = 0 \\ (u_{xx} + u_{yy})^2 + (v_{xx} + v_{yy})^2 = 1 \end{cases} \quad (1.2)$$

It now remains to substitute the sum of the third and fourth equations and the difference of the fifth and sixth equations into the last equation to obtain $0 = 1$. The equivalent polynomial system is

$$\begin{cases} z_1 + z_2 = 0 \\ z_3 - z_4 = 0 \\ z_5 + z_9 = 0 \\ z_6 - z_9 = 0 \\ z_{10} + z_8 = 0 \\ z_{10} - z_7 = 0 \\ (z_5 + z_6)^2 + (z_7 + z_8)^2 = 1 \end{cases}$$

which is inconsistent by the above reasoning. In this particular example, it is enough to differentiate the first two equations of (1.1) only once to discover that the corresponding polynomial system is inconsistent.

Our main result, Theorem 3.4, provides a uniform upper bound on the number of differentiations needed for all systems of polynomial PDEs with the number of derivations, indeterminates, total order, and total degree bounded by m , n , h , and d , respectively. This bound substantially outperforms the previously known general upper bound [8]. Our result reduces the problem to the polynomial effective Nullstellensatz, which has been very well studied, with many sharp results available (see, for example, [3, 6, 11, 14, 15] and the references given there). On the other hand, note that our problem is substantially more difficult than this problem, because the polynomial effective Nullstellensatz corresponds (see Theorem 4.3) to the effective differential Nullstellensatz restricted to systems of linear ($d = 1$) PDEs in one indeterminate ($n = 1$) with constant coefficients, and we do not make these restrictions.

The effective differential Nullstellensatz was first addressed in [19], without providing a complete solution. In the ordinary case ($m = 1$), the first bound, which was triple-exponential in n and polynomial in d appeared in [9]. The first general formula for the upper bound and first series of examples for the lower bound in the case of m derivations appeared in [8]. That formula is expressed in terms of the Ackermann function and is primitive recursive but not elementary recursive in n, h, d for each fixed m and is not primitive recursive in m . In the case of constant coefficients and $m = 1$, an important breakthrough was made in [5], where a double-exponential bound in n was given.

In the present paper, we go much beyond the final result of [5] and use the new methods discovered by logicians for fields with several commuting derivations [7, 18] to obtain a new upper bound for the most general case: the coefficients do not have to be constant and we allow any number m . For any m , our bound is polynomial in d . For $m = 1, 2$, a more concrete analysis of the bound is given in Section 3.3, which shows that our bound is elementary recursive in these cases. In particular, for $m = 1$, it is double-exponential in n and h and is polynomial in d , as in [5], but does not require constant coefficients. For $m = 2$, it is iterated exponential in h of length $n + 2$. Our Examples 4.2 and 4.6 show lower bounds that are polynomial in h and d and exponential in mn .

The paper is organized as follows. We begin in Section 2 with introducing the concepts and notation that we further use in the paper. Section 3 contains the main result of the paper, Theorem 3.4, as well as a discussion of the bound for small numbers of derivations in Section 3.3. The lower bound is given in Section 4.

2 Basic definitions

A detailed introduction to the subject can be found in [4, 12, 13, 16]. We will introduce only what is used in the paper. A *differential ring* (K, Δ) is a commutative ring K with a finite set $\Delta = \{\partial_1, \dots, \partial_m\}$ of pairwise commuting derivations on K . We let

$$\Theta = \left\{ \partial_1^{i_1} \cdot \dots \cdot \partial_m^{i_m} \mid i_j \geq 0, 1 \leq j \leq m \right\}.$$

For $\theta = \partial_1^{i_1} \cdot \dots \cdot \partial_m^{i_m}$, we let

$$\text{ord } \theta = i_1 + \dots + i_m.$$

Let also

$$R = K\{y_i \mid 1 \leq i \leq n\} := K[\theta y_i \mid \theta \in \Theta, 1 \leq i \leq n] \text{ and } R_h = K[\theta y_i \mid 1 \leq i \leq n, \text{ord } \theta \leq h], \quad h \geq 0.$$

The ring R defined above is called the *ring of differential polynomials* in differential indeterminates y_1, \dots, y_n and with coefficients in K . The ring R is naturally a differential ring. We will use, what we will call, an *orderly ranking* $>$ on Θ . This is a total order on Θ such that, for all $\theta_1, \theta_2 \in \Theta$, if $\text{ord } \theta_1 > \text{ord } \theta_2$, then $\theta_1 > \theta_2$. An example of such a ranking is given by ordering the n -tuples of exponents in Θ degree-lexicographically.

For a subset F of a ring R , (F) denotes the ideal generated by F and $\sqrt{(F)}$ denotes the radical ideal generated by F . For a subset F of a differential ring R , $[F]$ denotes the differential ideal generated by F in R and $\{F\}$ denotes the radical differential ideal generated by F in R . Note that, if $\mathbb{Q} \subset R$, then $\{F\} = \sqrt{[F]}$.

A field L is called *differentially closed* if, for every $F \subset L\{y_1, \dots, y_n\}$, the existence of a differential field $M \supset L$ and $(a_1, \dots, a_n) \in M^n$ such that, for all $f \in F$, $f(a_1, \dots, a_n) = 0$ implies the existence of $(b_1, \dots, b_n) \in L^n$ with, for all $f \in F$, $f(b_1, \dots, b_n) = 0$. In other words, L is differentially closed if and only if the inconsistency of a system of polynomial differential equations with coefficients in L is preserved under differential field extensions of L .

Let K be a differential field of characteristic zero. The *weak form of the differential Nullstellensatz* states that, for all $F \subset K\{y_1, \dots, y_n\}$, $1 \notin [F]$ if and only if, for all differentially closed fields $L \supset K$, there exists $(a_1, \dots, a_n) \in L^n$ such that, for all $f \in F$, $f(a_1, \dots, a_n) = 0$. The *strong form of the differential Nullstellensatz* states that for all $F \subset K\{y_1, \dots, y_n\}$ and $g \in K\{y_1, \dots, y_n\}$, $g \in \sqrt{[F]}$ if and only if, for all differentially closed fields $L \supset K$ and all $(a_1, \dots, a_n) \in L^n$ such that, for all $f \in F$, $f(a_1, \dots, a_n) = 0$, we have $g(a_1, \dots, a_n) = 0$.

3 Main result

We will start by showing several auxiliary results in Section 3.1. The main result, Theorem 3.4, is contained in Section 3.2. This is continued with an analysis of our estimate for particular numbers of derivations in Section 3.3.

3.1 Preparation

Let $l \geq 0$ and $J \subset R_l$ be an ideal. For each $k \in \mathbb{N}$, let $J^{(k)}$ be the ideal of the ring R_{l+k} generated by the derivatives of the elements of J up to order k (cf. [17]), that is,

$$J^{(k)} = (\theta g \mid g \in J, \text{ord } \theta \leq k).$$

For $D \in \Theta$, let $J^{(D)}$ be the ideal of $R_{l+\text{ord } D}$ generated by the derivatives of the elements of J not exceeding D in an orderly ranking, that is,

$$J^{(D)} = (\theta g \mid g \in J, \theta \leq D).$$

For every ideal J of the ring R_l , we let

$$J' = \sqrt{(\theta J \mid \text{ord } \theta \leq 1)} \cap R_l.$$

We also let

$$\alpha_l = \binom{l+m}{m}.$$

Note that

$$\dim_K R_l = n\alpha_l.$$

Lemma 3.1. *Let $J \subset R_l$ be an ideal, $p > 0$, and $(J')^p \subseteq J^{(1)}$. Then, for all $k \geq 0$,*

$$\sqrt{J^{(k)}} \subseteq \sqrt{J^{(kp+1)}}.$$

Proof. Fix an orderly ranking on the ring of Δ -polynomials $K\{y\}$. Let $D \in \Theta$, $p \in \mathbb{N}$. Then there exist $\beta_l \in K\{y\}$ such that

$$D^p(y^p) = (D(y))^p + \sum_{\theta(l)y < Dy} \beta_l \theta(l)y. \quad (3.1)$$

Indeed, let $D = \partial_1^{i_1} \dots \partial_m^{i_m} \in \Theta(r)$. By the Leibniz rule, for every weight- and degree-homogeneous differential polynomial z , the differential polynomial ∂z is homogeneous of degree equal to $\deg z$ and of weight with respect to ∂ equal to that of z plus one. Hence,

$$D^p(y^p) = \sum_{\substack{\sum_{k=1}^p l_1^k = pi_1, \dots, \sum_{k=1}^p l_m^k = pi_m}} c_{\mathbf{?}} \partial_1^{l_1^1} \dots \partial_m^{l_m^1} y \cdot \dots \cdot \partial_1^{l_1^p} \dots \partial_m^{l_m^p} y, \quad (3.2)$$

where $c_{\mathbf{?}}$ are some elements of K . Consider a monomial in the right-hand side of (3.2). Suppose that it is of order greater than r in every differential indeterminate that appears in it. Then, for each k , $1 \leq k \leq p$, we have

$$l_1^k + \dots + l_m^k > r.$$

Adding p inequalities, we obtain

$$pr = p(i_1 + \dots + i_m) = \sum_{k=1}^p \sum_{t=1}^m l_t^k > pr,$$

which is a contradiction. Therefore, for each monomial in the right-hand side of (3.2), one of the factors has order $\leq r$, and we have:

$$D^p(y^p) = \sum_{\substack{\Sigma_{k=1}^p l_1^k = pi_1, \dots, \Sigma_{k=1}^p l_m^k = pim \\ \Sigma_{k=1}^m l_1^1 \geq r, \dots, \Sigma_{k=1}^m l_p^p \geq r}} c_{\theta} \partial_1^{l_1^1} \dots \partial_m^{l_m^1} y \cdot \dots \cdot \partial_1^{l_1^p} \dots \partial_m^{l_m^p} y + \sum_{l < r} \beta_l \theta(l) y, \quad (3.3)$$

If, in a monomial from the first sum in (3.3), at least one of the factors had order greater than r , then, as in the above, by adding p inequalities, we would arrive at a contradiction. Thus, we obtain:

$$D^p(y^p) = \sum_{\substack{\Sigma_{k=1}^p l_1^k = pi_1, \dots, \Sigma_{k=1}^p l_m^k = pim \\ \Sigma_{k=1}^m l_1^1 = r, \dots, \Sigma_{k=1}^m l_p^p = r}} c_{\theta} \partial_1^{l_1^1} \dots \partial_m^{l_m^1} y \cdot \dots \cdot \partial_1^{l_1^p} \dots \partial_m^{l_m^p} y + \sum_{l < r} \beta_l \theta(l) y, \quad (3.4)$$

Let the ranking be such that $\partial_1 > \dots > \partial_m$ and, in the first sum in (3.4), for one of the factors, we have $l_1^k > i_1$ for all k , $1 \leq k \leq p$. Adding these p inequalities, we obtain

$$pi_1 = \sum_{k=1}^p l_1^k > pi_1,$$

which gives a contradiction. Thus,

$$D^p(y^p) = \sum_{\substack{\Sigma_{k=1}^p l_1^k = pi_1, \dots, \Sigma_{k=1}^p l_m^k = pim \\ \Sigma_{k=1}^m l_1^1 = r, \dots, \Sigma_{k=1}^m l_p^p = r \\ l_1^1 = i_1, \dots, l_1^p = i_1}} c_{\theta} \partial_1^{l_1^1} \dots \partial_m^{l_m^1} y \cdot \dots \cdot \partial_1^{l_1^p} \dots \partial_m^{l_m^p} y + \sum_{\theta(l) y < D y} \beta_l \theta(l) y,$$

As before, note that, for each monomial from the first sum, one cannot have $l_2^k > i_2$ for all k , $1 \leq k \leq p$. Therefore, in this sum, we are left with just the monomials of order $\leq r$ of the form

$$\partial_1^{i_1} \partial_2^{i_2} \partial_3^{l_3^1} \dots \partial_m^{l_m^1} y \cdot \partial_1^{i_1} \partial_2^{i_2} \partial_3^{l_3^p} \dots \partial_m^{l_m^p} y,$$

moving the rest of the monomials to the other sum. We now see that, distributing all monomials between these two sums accordingly, we obtain that the first sum contains only one summand and, therefore, obtain (3.1).

We will prove the statement of the lemma now. By induction on k , we will show that, for all $D \in \Theta$ of order k ,

$$\sqrt{J'(D)} \subseteq \sqrt{J^{(kp+1)}}.$$

For every $j' \in J'$, by the definition of J' , there exists $p \geq 1$ such that

$$j'^p = \theta j_0, \quad j_0 \in J, \quad \text{ord } \theta \leq 1. \quad (3.5)$$

Let $k = 0$, $D \in \Theta(0)$. By the definition of J' ,

$$\sqrt{J'} = J' \subseteq \sqrt{J^{(1)}},$$

and the statement holds. Consider an orderly ranking $<$ on the set of differential polynomials in one differential indeterminate and let, for all $D' < D$, $\text{ord } D' = k$,

$$\sqrt{J'(D')} \subseteq \sqrt{J^{(kp+1)}}.$$

By (3.1) for $y = j'$, (3.5) implies

$$(D(j'))^p + \sum_{D' < D} \beta_{D'} D' j' = D^p (\theta(1) j_0). \quad (3.6)$$

Since

$$D^p (\theta(1) j_0) \in J^{(kp+1)}$$

and, by the inductive hypothesis, a zero of $J^{(kp+1)}$ vanishes $D' j'$ in (3.6), we have

$$\sqrt{J^{(D)}} \subseteq \sqrt{J^{(kp+1)}}. \quad \square$$

Lemma 3.2. *Let $s \geq 0$,*

$$I_0 = (F_0) \subseteq I_1 = (F_1) \subseteq \dots \subseteq I_s = (F_s) \subseteq R_l$$

be ideals of R_l , $p_j \geq 0$, $0 \leq j \leq s$, and, for all i , $1 \leq i \leq s$,

$$I_i = (I_{i-1})' \quad \text{and} \quad I_i^{p_i} \subset I_{i-1}^{(1)}.$$

Then, for all $q \in \mathbb{N}$, there exists k such that

$$I_s^{(q)} \subseteq \sqrt{(F_0)^{(k)}} \quad \text{and} \quad k \leq 1 + p_1 + p_1 \cdot p_2 + \dots + q \cdot p_1 \cdot \dots \cdot p_s.$$

Proof. Let $g \in I_s^{(q)}$. Then $g \in I_{s-1}'^{(q)}$. Set $J = I_{s-1}$. Then

$$J^{(1)} = (F_{s-1}, \partial F_{s-1} \mid \partial \in \Delta), \quad J' = \sqrt{J^{(1)}} \cap R_l.$$

Applying Lemma 3.1 with $k = q$, we obtain

$$g \in \sqrt{I_{s-1}^{(qp_s+1)}}.$$

Again, by Lemma 3.1 with $k = qp_s + 1$ and $J = I_{s-1}$, we have

$$g \in \sqrt{I_{s-2}^{(p_{s-1}(qp_s+1)+1)}}.$$

Arguing similarly, we obtain

$$g \in \sqrt{I_0^{(1+\dots+(1+(p_s q)p_{s-1})\dots p_1)}} \subseteq \sqrt{(F_0)^{(1+\dots+(1+(qp_s)p_{s-1})\dots p_1)}}. \quad \square$$

For all $F \subset R_h$, we let (see [7, pages 15-16] for the recursive definition of $T_h^{m,n}$, which we do not give here, because it is lengthy)

$$I = \sqrt{(F)}, \quad T = T_h^{m,n}, \quad I_0 = \sqrt{I^{(T)}} \cap R_{T-1} \quad (3.7)$$

and

$$I_k = \sqrt{(g, \partial g \mid g \in I_{k-1}, \partial \in \Delta)} \cap R_{T-1} = \sqrt{I_{k-1}^{(1)}} \cap R_{T-1}. \quad (3.8)$$

Lemma 3.3 (cf. [7, Proposition 4.1]). *If $1 \in [F]$, then, for all $k \geq 1$ such that $I_k \neq R_{T-1}$,*

$$\dim I_{k-1} > \dim I_k.$$

Proof. Suppose that

$$\dim I_k = \dim I_{k-1} \quad (3.9)$$

for some $k \geq 1$. Fix such k . Since $I_{k-1} \subset I_k$, by (3.9), there exists a minimal prime component of I_k that is a minimal prime component of I_{k-1} . Pick such a component and denote it by Q . Let P be a prime component of $\sqrt{I_{k-1}^{(1)}} \subset R_T$ such that

$$Q = P \cap R_{T-1}, \quad (3.10)$$

which exists by [2, Proposition 16, Section 2, Chapter II]. Let

$$R_T/P = K \left[a_i^\theta \mid 1 \leq i \leq n, \text{ord } \theta \leq T \right].$$

Then, by (3.10),

$$R_{T-1}/Q = K[b], \quad b := \left(a_i^\theta \mid 1 \leq i \leq n, \text{ord } \theta < T \right).$$

We will show that the field

$$L = K \left(a_i^\theta \mid 1 \leq i \leq n, \text{ord } \theta \leq T \right)$$

satisfies the differential condition [18, page 10]. Indeed, it is sufficient to show that, for all k , $1 \leq k \leq m$, there exists a derivation $D_k : L' \rightarrow L$, where $L' = K(b)$, extending ∂_k so that

$$D_k a_i^\theta = a_i^{\partial_k \cdot \theta}$$

for all $a_i^\theta \in L'$. For this, it is sufficient to show that, if

$$f \in K \left[x_i^\theta \mid 1 \leq i \leq n, \text{ord } \theta \leq T-1 \right] \quad \text{and} \quad f(b) = 0,$$

then

$$\sum_{\substack{1 \leq i \leq n \\ \text{ord } \theta \leq T-1}} \frac{\partial f}{\partial x_i^\theta}(b) a_i^{\partial_k \cdot \theta} + f^{\partial_k}(b) = 0 \quad (3.11)$$

(here f^{∂_k} is the polynomial obtained from f by applying ∂_k to its coefficients.) Note that $Q^{(1)} \subset P$. Indeed, let J be the intersection of all minimal prime components of I_{k-1} not equal to Q , $h \in Q$, $\partial \in \Delta$, and $g \in J \setminus Q$ be such that $hg \in I_{k-1}$. By [12, Lemma 1.3, Chapter I],

$$g \cdot \partial h \in \sqrt{I_{k-1}^{(1)}} \subset P.$$

Since $g \notin Q$ and $g \in R_{T-1}$, $g \notin P$. Hence, $\partial h \in P$.

Finally, since $f(b) = 0$, $f \in Q$. Hence, $\partial f \in Q^{(1)} \subset P$, which implies (3.11). By the choice of T and [18, Theorem 4.10], if L satisfies the differential condition, $\text{Quot}(R/\{Q\})$ is a non-trivial extension of the differential field (K, Δ) , which contradicts $1 \in [F] \subset [I_k]$. \square

3.2 Main result

Theorem 3.4. *Let $h, D \geq 0$, $F \subset R_h$, $\deg F \leq D$. Then $1 \in [F]$ if and only if there exists $k \geq 0$ such that*

$$k \leq (n\alpha_{T-1}D)^{2^{O(n^3\alpha_T^3)}} \quad \text{and} \quad 1 \in (F)^{(k)},$$

where $\alpha_T = \binom{T+m}{m}$ and $T = T_h^{m,n}$ is recursively defined in [7, pages 15-16].

Proof. If $1 \in (F)^{(k)}$, then $1 \in [F]$ by definition. We will now show the reverse implication. Let $s = \dim Z(F)$ and also

$$a := n\alpha_{T-1}, \quad b := n\alpha_T, \quad c := O\left(n^2\alpha_{T-1}^2\right). \quad (3.12)$$

Then

$$\deg Z(F) = \deg Z(I) \leq D^s \leq D^{n\alpha_h}.$$

Hence, by [5, Proposition 4], the ideal I (as well as the ideal $I^{(T)}$) can be generated by polynomials of degree at most

$$(n\alpha_h D^s)^{2^{O(sn\alpha_h)}} \leq (n\alpha_h)^{2^{O(n^2\alpha_h^2)}} D^{n\alpha_h \cdot 2^{O(n^2\alpha_h^2)}} = (n\alpha_h D)^{2^{O(n^2\alpha_h^2)}} =: d_F.$$

Then

$$\deg Z(I_0) \leq d_F^{n\alpha_T} = (n\alpha_h D)^{b 2^{O(n^2\alpha_h^2)}} =: D_0$$

and the ideal I_0 can be generated by polynomials of degrees at most

$$(aD_0)^{2^c} = (a)^{2^c} (n\alpha_h D)^{b 2^{O(n^2\alpha_h^2)} + c} =: d_0.$$

Moreover, by [11, Theorem 1.3],

$$\sqrt{I^{(T)}}^{p_0} \subset I^{(T)}, \quad p_0 := d_F^b.$$

Hence,

$$I_0^{p_0} \subset I^{(T)} \cap R_{T-1}.$$

Continuing this way, we obtain that

$$\deg Z(I_{i+1}) \leq d_i^{n\alpha_T} =: D_{i+1}$$

and the ideal I_{i+1} can be generated by polynomials of degrees at most

$$d_{i+1} = a^{2^c} (d_i)^{b 2^c} = a^{2^c} \left(a^{2^c} d_{i-1}^{b 2^c}\right)^{b 2^c} = a^{2^c + b 2^{2c}} d_{i-1}^{b^2 2^{2c}} = a^{2^c + b 2^{2c}} \left(a^{2^c} d_{i-2}^{b 2^c}\right)^{b^2 2^{2c}} = a^{2^c + b 2^{2c} + b^2 2^{3c}} d_{i-2}^{b^3 2^{3c}}.$$

Therefore,

$$d_{i+1} = a^{2^c \sum_{j=0}^q (b 2^c)^j} d_{i-q}^{(b 2^c)^{q+1}} = a^{2^c \sum_{j=0}^i (b 2^c)^j} d_0^{(b 2^c)^{i+1}} = a^{2^c \frac{(b 2^c)^{i+1} - 1}{b 2^c - 1}} d_0^{(b 2^c)^{i+1}} \leq \left(a^{2^c} d_0\right)^{(b 2^c)^{i+1}}$$

and

$$D_{i+1} \leq \left(a^{2^c} d_0\right)^{b(b 2^c)^i}.$$

Again, by [11, Theorem 1.3],

$$\sqrt{I_i^{(1)}}^{p_{i+1}} \subset I_i^{(1)}, \quad p_{i+1} := \left(a^{2^c} d_0\right)^{b(b 2^c)^i} \geq d_i^b, \quad i \geq 0.$$

Hence,

$$I_{i+1}^{p_{i+1}} \subset I_i^{(1)} \cap R_{T-1}.$$

By Lemma 3.3, $1 \in I_a$. By Lemma 3.2 applied to (3.8),

$$1 \in I_0^{(1+p_1+p_1 \cdot p_2 + \dots + p_1 \cdot \dots \cdot p_a)}.$$

Again by Lemma 3.2, for all $q \geq 0$,

$$I_0^{(q)} \subset \sqrt{I^{(T+1+qp_0)}}.$$

Hence,

$$1 \in I^{(T+1+p_0(1+p_1+p_1 \cdot p_2 + \dots + p_1 \cdot \dots \cdot p_a))}.$$

By Lemma 3.1 again, we obtain

$$1 \in (F)^{(p_0(T+1+p_0(1+p_1+p_1 \cdot p_2+\dots+p_1 \cdot \dots \cdot p_a)))} = (F)^{(p_0(T+1+\dots(1+(1+p_a)p_{a-1})\dots p_0))} = (F)^{(p_0(T+p_0 \cdot \dots \cdot p_a))}, \quad (3.13)$$

with the latter equality following from the definition of c via the O -symbol. Note that

$$\begin{aligned} p_0^2 p_1 \cdot \dots \cdot p_a &= d_F^{2b} \left(a^{2^c} d_0 \right)^{b \sum_{j=0}^{a-1} (b2^c)^j} = d_F^{2b} \left(a^{2^c} d_0 \right)^{b \left(\frac{(b2^c)^a - 1}{b2^c - 1} - 1 \right)} \\ &\leq d_F^{2b} \left(a^{2^c} d_0 \right)^{b(b2^c)^a} = d_F^{2b} \left(a^2 d_F^b \right)^{(b2^c)^{a+1}} \\ &\leq (ad_F)^{b((b2^c)^{a+1}+2)} = (ad_F)^{2^{cb}} = a^{2^{cb}} (n\alpha_h D)^{2^{O(n^2 \alpha_h^2)} + cb} \\ &= a^{2^{cb}} (n\alpha_h D)^{2^{cb}} = (aD)^{2^{cb}}, \end{aligned}$$

(again, the equalities hold because of the O -definition of c and also because $\alpha_T \geq 1$ if $h \geq 1$ and $k = a = 0$ if $h = 0$) and the result now follows by substituting (3.12) in the above and using (3.13). \square

Corollary 3.5. (cf. [5, Corollary 21]) Let $h, D \geq 0$, $F \subset R_h$, $f \in R_h$, and $\max\{\deg f, \deg F\} \leq D$. Then $f \in \sqrt{[F]}$ if and only if there exists $k \geq 0$ such that

$$k \leq (n\alpha_{T'-1} D)^{2^{O(n^3 \alpha_{T'}^3)}} \quad \text{and} \quad f \in \sqrt{(F)^{(k)}},$$

where $T' := T_h^{m,n+1}$.

Proof. If $f \in \sqrt{(F)^{(k)}}$, then $f \in \sqrt{[F]}$ by definition. Let $f \in \sqrt{[F]}$. Then $1 \in [1 - tf, F] \subset K\{y_1, \dots, y_n, t\}$. By Theorem 3.4,

$$1 \in \left((1 - tf)^{(k)}, F^{(k)} \right),$$

for which we used the properties of O to go down from $D+1$ (which appears because $\deg tf = \deg f + 1$) to D and from $n+1$ to n outside of T' . As usual, by substituting $1/f$ into t and clearing out the denominators, we obtain the result. \square

Remark 3.6. Note that, for $m \geq 2$, $T \neq O(T')$ (see Section 3.3), and so we do not replace T' by T in the corollary. However, for $m = 1$, we simply have $T = T' = h$.

3.3 Concrete values of the number of derivations

According to [7, page 16], if $m = 1$, then $T = h$. Then the bound from Theorem 3.4 is

$$(nhD)^{2^{O(n^3 (h+1)^3)}}$$

and is better than the bound from [5, Corollary 19]. Indeed, our result holds for non-constant coefficients and also, if $h = 0$, then our bound naturally gives 0, but the bound from [5, Corollary 19] gives $(nD)^{2^{O(n^3)}}$. Of course, one can just prove directly that, if $h = 0$, then $k = 0$. If $m = 2$, by [7, Lemma 3.8],

$$T = T(n, h) = 2^{b_{n,h}+1} h, \quad b_{0,h} = 0, \quad b_{i+1,h} = 2^{b_i+1} h + b_i + 1.$$

Therefore, in this case, the bound from Theorem 3.4 is polynomial in D (as it is for arbitrary m , n , and h) and is iterated-exponential in h , with the length of the tower being equal to $n+2$.

For comparison, note that the bound from [8, Theorem 1], $A(m+8, \max(n, h, d))$, has a substantially higher growth rate, as, for example, $A(3, x)$ is exponential in x and $A(4, x)$ is a tower of exponentials of length $x+3$, and the minimal possible value here, $A(9, 1)$, is out of reach for any existing computer even to output.

4 Lower bound

The examples in [8] show that the lower bound for the effective differential Nullstellensatz is exponential in the number of variables and the number of derivations and polynomial in the degree of the system. We expand on these results, first by observing how the order of the system affects the lower bound.

Example 4.1. Consider the system $F = \{y_1^d, y_1 - y_2^d, \dots, y_{n-1} - y_n^d, 1 - y_n^{(h)}\} \subset K\{y_1, \dots, y_n\} =: R$ with one derivation. A particular and essential case of this, $h = 1$, was considered in an unpublished manuscript by York Kitajima, and the argument in the present example is based on Kitajima's argument and extends it, with extra subtleties. Recall that for $s \geq 2$ and $m, m_1, \dots, m_s \in \mathbb{N}$ with $m_1 + \dots + m_s = m$, the multinomial coefficient is

$$\binom{m}{m_1, \dots, m_s} = \frac{m!}{m_1! \cdots m_s!}.$$

For $l \geq 1$, denote by M_l the multinomial coefficient

$$M_l = \binom{d^l h}{d^{l-1} h, \dots, d^{l-1} h},$$

where this multinomial coefficient contains d terms. We claim that $(F)^{(j)} \subset I_j$ where

$$\begin{aligned} I_0 &= (y_1, y_2, \dots, y_{n-1}, y_n, 1 - y_n^{(h)}) \\ I_j &= (I_{j-1}, y_1^{(j)}, y_2^{(j)}, \dots, y_{n-1}^{(j)}, y_n^{(j)}, y_n^{(h+j)}) & 1 \leq j \leq h-1 \\ I_j &= (I_{j-1}, y_1^{(j)}, \dots, y_{n-i}^{(j)} - \prod_{l=1}^i M_l^{d^{i-l}}, y_{n-i+1}^{(j)}, \dots, y_{n-1}^{(j)}, y_n^{(h+j)}) & j = d^i h, 1 \leq i \leq n-1 \\ I_j &= (I_{j-1}, y_1^{(j)}, \dots, y_{n-1}^{(j)}, y_n^{(h+j)}) & \text{otherwise, } j \leq d^n h - 1. \end{aligned}$$

Indeed, we can show this by induction on j . The base case $j = 0$ is clear. Now assume $(F)^{(k)} \subset I_k$ for all $k < j$. By induction, we only need to show the inclusion of unmixed monomials, i.e. powers of a single derivative of a y_i . The generalized Leibniz rule says that for all $s \geq 1$, $m \geq 0$, and $f_1, \dots, f_s \in R$,

$$\left(\prod_{r=1}^s f_r \right)^{(m)} = \sum_{m_1 + \dots + m_s = m} \binom{m}{m_1, \dots, m_s} \prod_{r=1}^s f_r^{(m_r)}$$

In our system F , we have $s = d$. Unmixed monomials thus occur when $m_1 = \dots = m_d = m/d$. When $j \neq d^i h$, $y_i^{(j/d)} \in I_j$ for all i , $1 \leq i \leq n$, so there is nothing to prove. The case we must consider is when $j = d^i h$, in which case each m_α in the multinomial coefficient is $d^{i-1} h$ and $y_{n-i}^{(d^i h)} \notin I_{d^i h}$.

The only differential polynomial in $(F)^{(d^i h)}$ for which it remains to show that it is in $I_{d^i h}$ is $(y_{n-i} - y_{n-i+1}^d)^{(d^i h)}$, since $y_{n-i+1}^{(d^{i-1} h)} \notin I_{d^{i-1} h}$ by construction. Observe that

$$(y_{n-i} - y_{n-i+1}^d)^{(d^i h)} = y_{n-i}^{(d^i h)} - M_i (y_{n-i+1}^{(d^{i-1} h)})^d + g,$$

where $g \in K\{y\}$ contains no unmixed monomials, and so is in $I_{d^i h}$. Thus, it suffices to show that

$$y_{n-i}^{(d^i h)} - M_i (y_{n-i+1}^{(d^{i-1} h)})^d \in I_{d^i h}.$$

By construction,

$$y_{n-i+1}^{(d^{i-1}h)} - \prod_{l=1}^{i-1} M_l^{d^{i-l-1}} \in I_{d^{i-1}h} \subset I_{d^i h}.$$

We can thus write

$$\begin{aligned} y_{n-i}^{(d^i h)} - M_i \left(y_{n-i+1}^{(d^{i-1}h)} \right)^d = \\ \left(y_{n-i}^{(d^i h)} - \prod_{l=1}^i M_l^{d^{i-l}} \right) - M_i \sum_{\alpha=0}^{d-1} \left[\left(\prod_{l=1}^{i-1} M_l^{d^{i-l-1}} \right)^\alpha \left(y_{n-i+1}^{(d^{i-1}h)} \right)^{d-1-\alpha} \right] \left(y_{n-i+1}^{(d^{i-1}h)} - \prod_{l=1}^{i-1} M_l^{d^{i-l-1}} \right) \end{aligned}$$

in terms of elements of $I_{d^i h}$, completing the induction step and proving that $F^{(j)} \subset I_j$ for all j , $1 \leq j \leq d^n h - 1$.

Since $1 \notin I_j$ for all j , $0 \leq j \leq d^n h - 1$, then $1 \notin (F)^{(d^n h - 1)}$. Observe that

$$\begin{aligned} \left(y_n^{d^n} \right)^{(d^n h)} &= \left(\left(y_n^{d^n} \right)^{(h)} \right)^{((d^n - 1)h)} = \left(\left(\sum_{n_{1,1} + \dots + n_{1,d^n} = h} \binom{h}{n_{1,1}, \dots, n_{1,d^n}} \prod_{i=1}^{d^n} y_n^{(n_{1,i})} \right)^{(h)} \right)^{((d^n - 2)h)} \\ &= \left(\left(\sum_{n_{1,1} + \dots + n_{1,d^n} = h} \sum_{n_{2,1} + \dots + n_{2,d^n} = h} \binom{h}{n_{1,1}, \dots, n_{1,d^n}} \binom{h}{n_{2,1}, \dots, n_{2,d^n}} \prod_{i=1}^{d^n} y_n^{(n_{1,i} + n_{2,i})} \right)^{(h)} \right)^{((d^n - 3)h)} \\ &= \dots = \sum_{n_{1,1} + \dots + n_{1,d^n} = h} \dots \sum_{n_{d^n,1} + \dots + n_{d^n,d^n} = h} \left(\prod_{j=1}^{d^n} \binom{h}{n_{j,1}, \dots, n_{j,d^n}} \prod_{i=1}^{d^n} y_n^{(n_{1,i} + \dots + n_{d^n,i})} \right). \end{aligned}$$

Since $y_n^{(h)} \equiv 1$ modulo the system F , then $y_n^{(l)} \equiv 0$ for all $l > h$, so the only non-zero terms in this sum will be powers of $y_n^{(h)}$. We thus have that, modulo F , $\left(y_n^{d^n} \right)^{(d^n h)} \equiv 1$, so $1 \in (F)^{(d^n h)}$ and $1 \notin (F)^{(d^n h - 1)}$.

Example 4.2. Consider the following collections of differential polynomials in $K\{y_1, \dots, y_n\}$ with derivatives $\Delta = \{\partial_1, \dots, \partial_m\}$, with $d, h \geq 1$:

$$\begin{aligned} G_1 &= \left\{ (\partial_1 y_1)^d, \partial_1 y_1 - (\partial_2 y_1)^d, \dots, \partial_{m-1} y_1 - (\partial_m y_1)^d \right\} \\ G_i &= \left\{ \partial_m y_{i-1} - (\partial_1 y_i)^d, \partial_1 y_i - (\partial_2 y_i)^d, \dots, \partial_{m-1} y_i - (\partial_m y_i)^d \right\} \quad 1 \leq i \leq n-1 \\ G_n &= \left\{ \partial_m y_{n-1} - (\partial_1 y_n)^d, \partial_1 y_n - (\partial_2 y_n)^d, \dots, \partial_{m-1} y_n - (\partial_m y_n)^d, 1 - \partial_m^{h+1} y_n \right\}. \end{aligned}$$

Similar to what is done in [8], if we replace F in the previous example by $G = \bigcup_{i=1}^n G_i$, then the elements of G will need to be differentiated a minimum of $d^{mn}h$ times in order to reduce the system to 1, so $1 \in (G)^{(d^{mn}h)}$ and $1 \notin (G)^{(d^{mn}h - 1)}$.

In these examples, we see that the lower bound for having $f \in (G)^{(k)}$ is exponential in the number of derivations and number of variables and linear in the order of the system. However, these known examples are non-linear. We will use the lower bound on the effective polynomial Nullstellensatz to construct an example of a linear system $G \subset K\{y_1, \dots, y_n\}$ with $f \in (G)^{(k)}$ but $f \notin (G)^{(k-1)}$, where k is exponential in the number of derivations and the number of variables and polynomial in the order of the system.

We use a system of polynomials to construct a system of differential polynomials. We begin with polynomials in $K[X_1, \dots, X_m]$ and construct differential polynomials in $K\{y\}$ with derivatives $\Delta = \{\partial_1, \dots, \partial_m\}$, where K is constant with respect to each ∂_i . Given $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{N}^m$, denote $X^\alpha = X_1^{\alpha_1} \dots X_m^{\alpha_m}$ and $\partial^\alpha = \partial_1^{\alpha_1} \dots \partial_m^{\alpha_m}$.

Suppose we have $f_1, \dots, f_r \in K[X_1, \dots, X_m]$. For each i , $1 \leq i \leq r$, there exist $\alpha_{i,1}, \dots, \alpha_{i,N_i} \in \mathbb{N}^m$ and $c_{i,1}, \dots, c_{i,N_i} \in K$ such that

$$f_i = \sum_{j=1}^{N_i} c_{i,j} X^{\alpha_{i,j}}.$$

We then define $\tilde{f}_i \in K\{y\}$ to be

$$\tilde{f}_i = \sum_{j=1}^{N_i} c_{i,j} \partial^{\alpha_{i,j}} y.$$

Similarly, given $f = \sum_{j=1}^N s_j X^{\gamma_j} \in K[X_1, \dots, X_m]$, we can define $\tilde{f} = \sum_{j=1}^N s_j \partial^{\gamma_j} y \in K\{y\}$. Consider the system $G = \{\tilde{f}_1, \dots, \tilde{f}_r\}$.

Theorem 4.3. *Let $f, f_1, \dots, f_r \in K[X_1, \dots, X_m]$, $\tilde{f}, \tilde{f}_1, \dots, \tilde{f}_r \in K\{y\}$, and $G \subset K\{y\}$ be defined as above. Suppose $f \in (f_1, \dots, f_r)$ and let k be the lower bound for the degree of the coefficients of the f_i in any possible representation of f . Then $\tilde{f} \in (G)^{(k)}$ but $\tilde{f} \notin (G)^{(k-1)}$.*

Proof. Suppose $f \in (f_1, \dots, f_r)$, so there exist $g_1, \dots, g_r \in K[X_1, \dots, X_m]$ such that $f = g_1 f_1 + \dots + g_r f_r$. As with the f_i s, there exist $\beta_{i,j} \in \mathbb{N}^m$ and $d_{i,j} \in K$, $j = 1, \dots, M_i$, such that we can write each g_i as

$$g_i = \sum_{j=1}^{M_i} d_{i,j} X^{\beta_{i,j}}.$$

It is then easy to see that

$$\sum_{j=1}^{M_1} d_{1,j} \partial^{\beta_{1,j}} (\tilde{f}_1) + \dots + \sum_{j=1}^{M_r} d_{r,j} \partial^{\beta_{r,j}} (\tilde{f}_r) = \sum_{j=1}^N s_j \partial^{\gamma_j} y = \tilde{f}. \quad (4.1)$$

Since $G = \{\tilde{f}_1, \dots, \tilde{f}_r\}$, we thus have that $\tilde{f} \in [G]$, and since the maximum degree of the g_i s is k , the maximum order of the $\partial^{\beta_{i,j}}$ s is also k , so $\tilde{f} \in (G)^{(k)}$.

It remains to show that $\tilde{f} \notin (G)^{(k-1)}$. Suppose for a contradiction we have $\tilde{f} \in (G)^{(l)}$ for some $l < k$, so we can write

$$\tilde{f} = \sum_{j=1}^{K_1} \alpha_{1,j}(y) \partial^{\sigma_{1,j}} (\tilde{f}_1) + \dots + \sum_{j=1}^{K_r} \alpha_{r,j}(y) \partial^{\sigma_{r,j}} (\tilde{f}_r) \quad (4.2)$$

where the $\alpha_{i,j} \in K\{y\}$ and $\text{ord} \partial^{\sigma_{i,j}} \leq l < k$.

To complete the proof, we need the following fact about systems of homogeneous degree 1 polynomials. Suppose $p, p_1, \dots, p_s \in K[X_1, \dots, X_n]$ are homogeneous degree 1 polynomials. If there exist $q_1, \dots, q_s \in K[X_1, \dots, X_n]$ such that $p = q_1 p_1 + \dots + q_s p_s$, then we can in fact assume that all of the q_i are constant. Indeed, write $p = a_1 X_1 + \dots + a_n X_n$. Assume without loss of generality that $a_n \neq 0$. Since $p = q_1 p_1 + \dots + q_s p_s$, then

$$X_n = q_0 + \frac{q_1}{a_n} p_1 + \dots + \frac{q_s}{a_n} p_s, \quad q_0 := -\frac{a_1}{a_n} X_1 - \dots - \frac{a_{n-1}}{a_n} X_{n-1}.$$

Thus, it suffices to prove the result when $p = X_n$.

For this, we order the variables so that $X_1 > \dots > X_n$. Applying the Gauss-Jordan elimination to the system $\{p_i = 0\}$, we obtain a new system $\{p'_i = 0\}$ that is in reduced row echelon form. Moreover, every p'_i is a linear combination of p_1, \dots, p_r (with coefficients in K) and vice versa. There are two cases to consider. If X_n is a leading variable in $\{p'_i = 0\}$, then because of the ordering on the X_i , we must have in fact that X_n is one of the p'_i , and so the proof is complete.

Therefore, suppose X_n is not a leading variable of $\{p'_i = 0\}$. By assumption, $X_n \in (p_1, \dots, p_s) = (p'_1, \dots, p'_s)$. This implies that for every solution $(\alpha_1, \dots, \alpha_n)$ of the system $\{p_i = 0\}$ (or equivalently $\{p'_i = 0\}$), $\alpha_n = 0$. Thus,

X_n cannot be a free variable of $\{p'_i = 0\}$, since there is a solution of the system $\{p'_i = 0\}$ for every possible value of any free variable (provided that a solution exists, which in this case is true, given by $(0, \dots, 0)$).

Now, since the $\partial^{Y_j} y$ and $\partial^{\sigma_{i,j}}(\tilde{f}_i)$ in (4.2) are all homogeneous of degree 1, by the above discussion, we can assume that the $\alpha_{i,j}$ are all constants $b_{i,j} \in K$, so we obtain

$$\tilde{f} = \sum_{j=1}^{K_1} b_{1,j} \partial^{\sigma_{1,j}}(\tilde{f}_1) + \dots + \sum_{j=1}^{K_r} b_{r,j} \partial^{\sigma_{r,j}}(\tilde{f}_r). \quad (4.3)$$

Let

$$h_i = \sum_{j=1}^{K_i} b_{i,j} X^{\sigma_{i,j}}.$$

Based on our construction of (4.1) we can go backwards and deduce, using (4.3), that $f = h_1 f_1 + \dots + h_r f_r$. Since we know that $\text{ord} \partial^{\sigma_{i,j}} \leq l$, this means that $\deg h_i \leq l$, $1 \leq i \leq r$, contradicting the fact that the maximum degree must be at least $k > l$. \square

Remark 4.4. If $f = 1$ in Theorem 4.3, then $\tilde{f} = y$. Thus, by considering the system $G_1 = \{G, 1 - ty\} \subset K\{t, y\}$, we have $1 \in (G_1)^{(k)}$ and $1 \notin (G_1)^{(k-1)}$.

Example 4.5. For $m \geq 2$, consider the following system of polynomial equations in $K[X_1, \dots, X_m]$; cf. [3, page 578]:

$$f_1 = X_1^h, f_2 = X_1 - X_2^h, \dots, f_{m-1} = X_{m-2} - X_{m-1}^h, f_m = 1 - X_{m-1} X_m^{h-1}.$$

It is shown that $1 \in (f_1, \dots, f_m)$ and if $1 = g_1 f_1 + \dots + g_m f_m$, then

$$\deg(g_1) \geq h^m - h^{m-1} = h^{m-1}(h-1).$$

Thus, if k is the maximum degree of the g_i (that is smallest possible over the collection of all g_i so that $1 = \sum g_i f_i$), we must have that $k \geq h^{m-1}(h-1)$.

Let us use this polynomial system to create a system of differential polynomial in $K\{y\}$ with derivations $\Delta = \{\partial_1, \dots, \partial_m\}$. Let G be the system in $K\{y\}$ given by

$$\tilde{f}_1 = \partial_1^h y, \tilde{f}_2 = \partial_1 y - \partial_2^h y, \dots, \tilde{f}_{m-1} = \partial_{m-2} y - \partial_{m-1}^h y, \tilde{f}_m = y - \partial_{m-1} \partial_m^h y. \quad (4.4)$$

By the above discussion, we have $y \in (G)^{(k)}$ where $k \geq h^{m-1}(h-1)$ and $y \notin (G)^{(h^{m-1}(h-1)-1)}$. We have thus constructed a linear system G in which the number of derivations of the elements of G needed is exponential in the number of derivatives and polynomial in the order of the system.

We can construct an explicit linear combination of the \tilde{f}_i s and their derivatives equaling y that requires exactly $h^{m-1}(h-1)$ derivations of \tilde{f}_1 . Explicit g_i s are constructed in [3] such that $1 = g_1 f_1 + \dots + g_m f_m$ and $\deg(g_1) = h^{m-1}(h-1)$ by observing that, setting $D = h^{m-1}(h-1)$,

$$X_m^D (X_1^h) - \sum_{i=2}^{m-1} X_m^D \left(X_{i-1}^{h^{i-1}} - (X_i^h)^{h^{i-1}} \right) + \left(1 - (X_{m-1} X_m^{h-1})^{h^{m-1}} \right) = 1. \quad (4.5)$$

Thus, if we set

$$\begin{aligned} g_1 &= X_m^D \\ g_i &= X_m^D \left(\sum_{j=0}^{h^{i-1}-1} X_{i-1}^{h^{i-1}-1-j} (X_i^h)^j \right) \quad 2 \leq i \leq m-1 \\ g_n &= \sum_{j=0}^{h^{m-1}-1} (X_{m-1} X_m^{h-1})^j, \end{aligned}$$

then using (4.5), we have $1 = g_1 f_1 + \dots + g_m f_m$.

We can use these g_i s to find the desired linear combination of the \tilde{f}_i s and their derivatives. Using the corresponding identities in $K[X_1, \dots, X_m]$, we obtain that

$$\begin{aligned} \partial_{i-1}^{h^{i-1}} y - \partial_i^{h^i} y &= \sum_{j=0}^{h^{i-1}-1} \partial_{i-1}^{h^{i-1}-j-1} \partial_i^{h^j} (f_i) \quad 2 \leq i \leq m-1 \\ y - \partial_{m-1}^{h^{m-1}} \partial_m^{h^{m-1}(h-1)} y &= \sum_{j=0}^{h^{m-1}-1} \partial_{m-1}^j \partial_m^{j(h-1)} (f_m). \end{aligned}$$

Thus, setting $D = h^{m-1}(h-1)$, we can directly adapt (4.5) to see that

$$\partial_m^D (\partial_1^h y) - \sum_{i=2}^{m-1} \partial_m^D (\partial_{i-1}^{h^{i-1}} y - \partial_i^{h^i} y) + (y - \partial_{m-1}^{h^{m-1}} \partial_m^{h^{m-1}(h-1)} y) = y. \quad (4.6)$$

This gives us a linear combination of the \tilde{f}_i s and their derivatives that requires exactly $h^{m-1}(h-1)$ derivations of \tilde{f}_1 , which we know is minimal by the polynomial case.

Example 4.6. We can use (4.6) to generalize this result to the case of multiple variables. We will define a system in $K\{y_1, \dots, y_n\}$ with derivatives $\Delta = \{\partial_1, \dots, \partial_m\}$. Let $m \geq 2$. For $n = 1$, we have (4.4). For $n \geq 2$, consider the collection of differential polynomials:

$$\begin{aligned} G_1 &= \{\partial_1^h y_1, \partial_1 y_1 - \partial_2^h y_1, \partial_2 y_1 - \partial_3^h y_1, \dots, \partial_{m-2} y_1 - \partial_{m-1}^h y_1\} \\ G_i &= \{\partial_{m-1} y_{i-1} - \partial_1^h y_i, \partial_1 y_i - \partial_2^h y_i, \dots, \partial_{m-2} y_i - \partial_{m-1}^h y_i\} \quad 2 \leq i \leq n-1 \\ G_n &= \{\partial_{m-1} y_{n-1} - \partial_1^h y_n, \partial_1 y_n - \partial_2^h y_n, \dots, \partial_{m-2} y_n - \partial_{m-1}^h y_n, y_n - \partial_{m-1} \partial_m^h y_n\}. \end{aligned}$$

Then let $G = \bigcup_{i=1}^n G_i$. We claim that $y_n \in (G)^{(k)}$ where $k \geq h^{n(m-1)}(h-1)$ and

$$y_n \notin (G)^{(h^{n(m-1)}(h-1)-1)}. \quad (4.7)$$

We can write a system similar to the one in (4.6) to produce y_n in terms of the elements of G and their derivatives needing exactly $h^{n(m-1)}(h-1)$ derivations of $\partial_1^h y_1$. Let $E = h^{n(m-1)}(h-1)$. Then we have

$$\begin{aligned} \partial_m^E (\partial_1^h y_1) - \sum_{j=1}^n \sum_{i=2}^{m-1} \partial_m^E (\partial_{i-1}^{h^{(j-1)(m-1)+i-1}} y_j - \partial_i^{h^{(j-1)(m-1)+i}} y_j) \\ - \sum_{j=1}^{n-1} \partial_m^E (\partial_{m-1}^{h^{j(m-1)}} y_j - \partial_1^{h^{j(m-1)+1}} y_{j+1}) + (y_n - \partial_{m-1}^{h^{n(m-1)}} \partial_m^{h^{n(m-1)}(h-1)} y_n) = y_n. \end{aligned}$$

By the same argument that shows the minimality of $h^{m-1}(h-1)$ in Example 4.5, we know that we must differentiate $\partial_1^h y_1$ at least E times. This shows (4.7) and there is a $k \geq E$ with $y_n \in (G)^{(k)}$.

References

- [1] F. Boulier, F. Ollivier, D. Lazard, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 20(1): 73–121, 2009. URL <http://dx.doi.org/10.1007/s00200-009-0091-7>.

- [2] N. Bourbaki. *Algèbre commutative. Chapitres 1 à 4*. Éléments de Mathématique. Springer, 2006. URL <http://dx.doi.org/10.1007/978-3-540-33976-2>.
- [3] W.D. Brownawell. Bounds for the degrees in the Nullstellensatz. *Annals of Mathematics*, 126(3):577–591, 1987. URL <http://dx.doi.org/10.2307/1971361>.
- [4] A. Buium. *Differential algebra and Diophantine geometry*. Hermann, Paris, 1994.
- [5] L. D’Alfonso, G. Jeronimo, and P. Solernó. Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients. *Journal of Complexity*, 30(5):588–603, 2014. URL <http://dx.doi.org/10.1016/j.jco.2014.01.001>.
- [6] T. Dubé. A combinatorial proof of the effective Nullstellensatz. *Journal of Symbolic Computation*, 15(3): 277–296, 1993. URL <http://dx.doi.org/10.1006/jSCO.1993.1020>.
- [7] J. Freitag and O. León Sánchez. Effective uniform bounds in partial differential fields. 2014. URL <http://arxiv.org/abs/1411.0029>.
- [8] O. Golubitsky, M. Kondratieva, A. Ovchinnikov, and A. Szanto. A bound for orders in differential Nullstellensatz. *Journal of Algebra*, 322(11):3852–3877, 2009. URL <http://dx.doi.org/10.1016/j.jalgebra.2009.05.032>.
- [9] D. Grigoriev. Complexity of quantifier elimination in the theory of ordinary differential equations. *Lecture Notes Computer Science*, 378:11–25, 1989. URL http://dx.doi.org/10.1007/3-540-51517-8_81.
- [10] E. Hubert. Factorization-free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4-5):641–662, 2000. URL <http://dx.doi.org/10.1006/jSCO.1999.0344>.
- [11] Z. Jelonek. On the effective Nullstellensatz. *Inventiones Mathematicae*, 162(1):1–17, 2005. URL <http://dx.doi.org/10.1007/s00222-004-0434-8>.
- [12] I. Kaplansky. *An Introduction to Differential Algebra*. Hermann, Paris, 1957.
- [13] E. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.
- [14] J. Kollár. Sharp effective Nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988. URL <http://dx.doi.org/10.1090/S0894-0347-1988-0944576-7>.
- [15] T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Mathematical Journal*, 109(3):521–598, 2001. URL <http://dx.doi.org/10.1215/S0012-7094-01-10934-4>.
- [16] D. Marker. Model theory of differential fields. In *Model Theory of Fields*, pages 38–113. Springer, Berlin, 1996. URL <http://projecteuclid.org/euclid.lnl/1235423156>.
- [17] R. Moosa and T. Scanlon. Jet and prolongation spaces. *Journal of the Institute of Mathematics of Jussieu*, 9(2):391–430, 2010. URL <http://dx.doi.org/10.1017/S1474748010000010>.
- [18] D. Pierce. Fields with several commuting derivations. *Journal of Symbolic Logic*, 79(1):1–19, 2014. URL <http://dx.doi.org/10.1017/jSL.2013.19>.
- [19] A. Seidenberg. An elimination theory for differential algebra. *University of California publications in Mathematics*, III(2):31–66, 1956.